PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-101042

(43)Date of publication of application : 19.04.1989

(51)Int.Cl. H04L 9/00

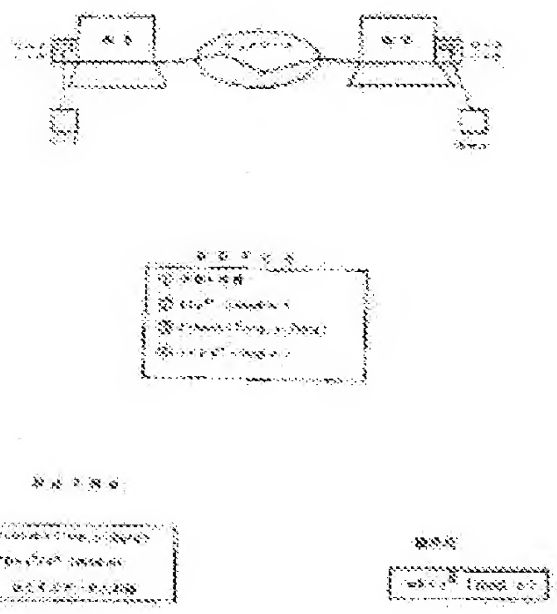
(21)Application number : 62-259023

(22)Date of filing : 13.10.1987

(71)Applicant : NEC CORP

(72)Inventor : OKAMOTO EIJI

(54) AUTHENTICATION DEVICE



(57)Abstract:

PURPOSE: To prevent a dishonest resending by a third party by preparing integers dependent of a time and an authenticator and providing a deciding means to decide whether the identification information of a sending side is made or not.

CONSTITUTION: To each user, a card, onto which integers (n), α, e1 and Si of the degree of 512 bits are written, is distributed from a card publisher or a center. Only the Si is the secret integer different for each user, and the others are common to each user. In forming an authenticator, a random number (r) is generated, and $x=\alpha^{e}r \pmod n$ is calculated from (e), α and (n) read out of the card of the user. Next, the hash function value of data Data to be transmit ted, a time Time and an above-mentioned integer (x), C=hash(Time, x, Data) is calculated. Next, whether a sent authenticator (x, y) and $Ye/xc1 \pmod n$ such as the (e), (n) and (x) from the card of the receiving side user are equal to an ID information ID1 of the transmitting side user or not is decided.

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平1－101042

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　平成1年(1989)4月19日
H 04 L 9/00		A－7240－5K	

審査請求　未請求　発明の数 3　（全4頁）

⑤4発明の名称　認証装置

⑳特　願　昭62－259023

㉒出　願　昭62(1987)10月13日

⑦2発明者　岡本　栄司　東京都港区芝5丁目33番1号　日本電気株式会社内

⑦1出願人　日本電気株式会社　東京都港区芝5丁目33番1号

⑦4代理人　弁理士　内原　晋

明細書

発明の名称　認証装置

特許請求の範囲

1．認証子を作成する認証装置において、ランダムな整数ｒを生成する乱数生成手段と、あらかじめ定められた複数の整数を記憶する記憶手段と、少なくとも時刻と前記乱数とに依存した整数ｃを生成するハッシュ化手段と、前記の複数の整数とｃ、ｒから認証子を生成する認証子生成手段と、から成ることを特徴とする認証装置。

2．あらかじめ定められた複数の整数とランダムに選んだ整数ｒと少なくとも時刻と該乱数に依存した整数ｃから作成した認証子を送り側から受取り、認証を行なう認証装置において、少なくとも時刻と前記認証子に依存した整数c_1を生成するハッシュ化手段と、前もって定められた複数の整数を記憶する記憶手段と、該整数と認証子とc_1からあらかじめ定められた変換を施した結果が送り側の識別情報になっているか否かを判定する判定手段と、から成ることを特徴とする認証装置。

3．通信相手に送るべき認証子を作成し、鍵を作成する認証装置において、ランダムな整数ｒを生成する乱数手段と、あらかじめ定められた複数の整数を記憶する記憶手段と、少なくとも時刻と前記乱数とに依存した整数ｃを生成するハッシュ化手段と、前記複数の整数とｃ、ｒから認証子を生成する認証子生成手段と、通信相手から送られた認証子が正しければそれと前記ｒを用いて鍵を生成する鍵生成手段と、から成ることを特徴とする認証装置。

発明の詳細な説明

（産業上の利用分野）

本発明はネットワークにおいて、通信相手ユーザあるいはメッセージの認証さらには通信の略号化に関する。

（従来の技術）

認証方式としてエー・シャミア(A.Shamir)がクリプト８４(Crypt

o'84)で提案した方式は、各ユーザの氏名などのＩＤ情報を用いた実用的方式として評価が高い。

（発明が解決しようとする問題点）

シャミアの方式には次の２つの欠点がある。１つは、正当なユーザから別の正当なユーザへの送信文を第３者が録音しておき、後にそれを再生送信すると受信者がその不正を検出できないことである。さらにもう１つは暗号通信と組合せようとすると、その鍵を送るための情報帯域が新たに必要となる。

（問題点を解決するための手段）

本発明によれば、認証子を作成する認証装置において、ランダムな整数ｒを生成する乱数生成手段と、あらかじめ定められた４つの整数ｎ、α、ｅ、ｓを記憶する記憶手段と、少なくとも時刻と前記乱数とに依存した整数ｃを生成するハッシュ化手段と、前記の整数ｎ、α、ｅ、ｓ、ｃ、ｒから２つの整数$\alpha^{er}(\mathrm{mod}\ n)$と$S\cdot\alpha^{cr}(\mathrm{mod}\ n)$から成る認証子を生成する認証子生成手段と、から成ることを特徴とする認証装置が得られる。

また、本発明によれば、あらかじめ定められた４つの整数ｎ、α、ｅ、ｓとランダムに選んだ整数ｒと少なくとも時刻に依存した整数ｃから作成した２つの整数$\alpha^{er}(\mathrm{mod}\ n)$と$S\cdot\alpha^{cr}(\mathrm{mod}\ n)$から成る認証子（ｘ，ｙ）を送り側から受取り、認証を行なう認証装置において、少なくとも時刻と前記認証子に依存した整数c_1を生成するハッシュ手段と、前記整数ｎとｅを記憶する記憶手段と、前記整数ｎ、ｅ、ｘ、ｙ、c_1に対して$y^e/x^{c_1}(\mathrm{mod}\ n)$が送り側の識別情報になっているか否かを判定する判定手段と、から成ることを特徴とする認証装置が得られる。

さらに本発明によれば、通信相手に送るべき認証子を作成し、鍵を生成する認証装置において、ランダムな整数ｒを生成する乱数生成手段と、あらかじめ定められた４つの整数ｎ、α、ｅ、ｓを記憶する記憶手段と、少なくとも時刻と前記乱数に依存した整数ｃを生成するハッシュ化手段と、前記の整数ｎ、α、ｅ、ｓ、ｃ、ｒから２つの整数$\alpha^{er}(\mathrm{mod}\ n)$と$S\cdot\alpha^{cr}(\mathrm{mod}\ n)$から成る認証子を生成する認証子生成手段と、通信相手から送られた認証子が正しければそれと前記整数ｒを用いて鍵を生成する鍵手段とから成ることを特徴とする認証装置が得られる。

（作用）

第１図は本発明の作用・原理を示すごく大まかな流れ図である。以下、認証子を作成する側を証明側、認証子を検証する側を認証側とよぶことにする。証明側は、認証側が検証を行えるような認証子を作成して他の必要なデータと共に送る。これが第１図(a)である。一方、認証側では送られた認証子の正否を判断する。これが第１図(b)である。さらに、受信側では暗号用の鍵を該認証子を用いて秘密に作成することができ、これが第1図(c)である。暗号通信の相手側も同じ略号用の鍵を持たなくてはならないが、これは受信側が(a)の証明側となって認証子を送信側に送り、該送信側が認証側となって(c)を実行すればよい。

（実施例）

第２図は本発明の一実施例を示す構成図である。ネットワークを介して接続されている端末の１つを送信ユーザが利用し、別の１つを受信ユーザが利用するものとする。各端末にはカードリーダが設置され、端末には認証のためのソフトあるいはハードが組込まれ、第１図を実行する。各ユーザには５１２ビット程度の整数ｎ、α、e_i、Ｓｉが書込まれたカードがカード発行者（又はセンター）から配布される。ここでS_iのみがユーザ毎に異なる秘密の整数で他は各ユーザに共通である。ユーザｉのＩＤ情報をID_iとすると、Ｓｉは

$$S_i^e\ (\mathrm{mod}\ n) = ID_i$$

を満たすように作られている。このようにできることは、コミュニケーション・オブ・ザ・エーシーエム(Communication of the ACM)第21巻 2号120頁～126頁に示されている。

端末がなすべき作業は第１図に示してあるが、その中の認証子作成、認証子検証、鍵生成の実施例を各々第３、４、５図に示す。

認証子作成では乱数ｒを生成し、ユーザのカー

ドから読出したｅ、α、ｎからｘ＝α^{er}(mod n)を計算する。次々に送るべきデータＤａｔａと時刻Ｔｉｍｅと前記整数ｘのハッシュ関数値、Ｃ＝ｈａｓｈ(Time,x,Data)を計算する。ここでハッシュ関数ｈａｓｈは例えばアイイーイーイー(IEEE)の確認コンピュータ(COMPUTER)誌1983年 2同号55頁～62頁に記載されている関数である。Ｄａｔａは謂ゆるメッセージ以外にも送信者のＩＤ情報やその他のデータを含めてもよい。このとき、認証子（ｘ，ｙ）は上記ｘと

ｙ＝Ｓｉ・d^{cr}（ｍｏｄ　ｎ）

で与えられる。Ｓｉもユーザのカードから読み出した整数である。

第４図の認証子検証では前記ハッシュ関数により同様にｃ＝ｈａｓｈ(Time,x,Data)を計算する。ここでＤａｔａは送信側から送られたデータであり、Ｔｉｍｅは送信側が認証子作成の際に用いた時刻情報であり、受信側で正しくわからない場合にはＴｉｍｅを送ってもらう必要がある。ｘは送られた認証子の一部である。次に送られて認証子（ｘ，ｙ）と受信側ユーザのカードからのｅ、ｎ、ｘ、ら

y^e / x^c（ｍｏｄ　ｎ）

が送信側ユーザのＩＤ情報ＩＤｉに等しいか否かを判定する。もし等しくなければ不正データとみなす。送信側ユーザが送った（ｘ，ｙ）を用いれば、ｘ，ｙの定義から、ｎを法として

$y^e / x^c = Si^e \alpha^{cre} / \alpha^{erc} = ID_i$

となる。

第５図の鍵生成では、乱数Ｒを用いて、

$WK = X^R$（ｍｏｄ　ｎ）

により作成する。ここでｘは認証側から送られたものであり、乱数Ｒは認証子作成に用いた乱数である。即ち、受信側でも鍵生成の場合には（作用）の項で述べたように認証子作成を行なうが、その時に用いた乱数Ｒである。送信側でも認証子作成に用いた乱数ｒを鍵生成に用いる。いずれの側でもＷＫはα^{erR}(mod n)に等しくなる。

以上の実施例において、巾乗剰除ｚ＝a^b(mod n)の計算は端末のソフトで行なうことも、プロセッサで行なうこともできる。また、時刻情報Ｔｉｍｅは時刻そのものではなく、毎回異なるようなビットパターンでもよく、時刻により変わるものならよい。

（発明の効果）

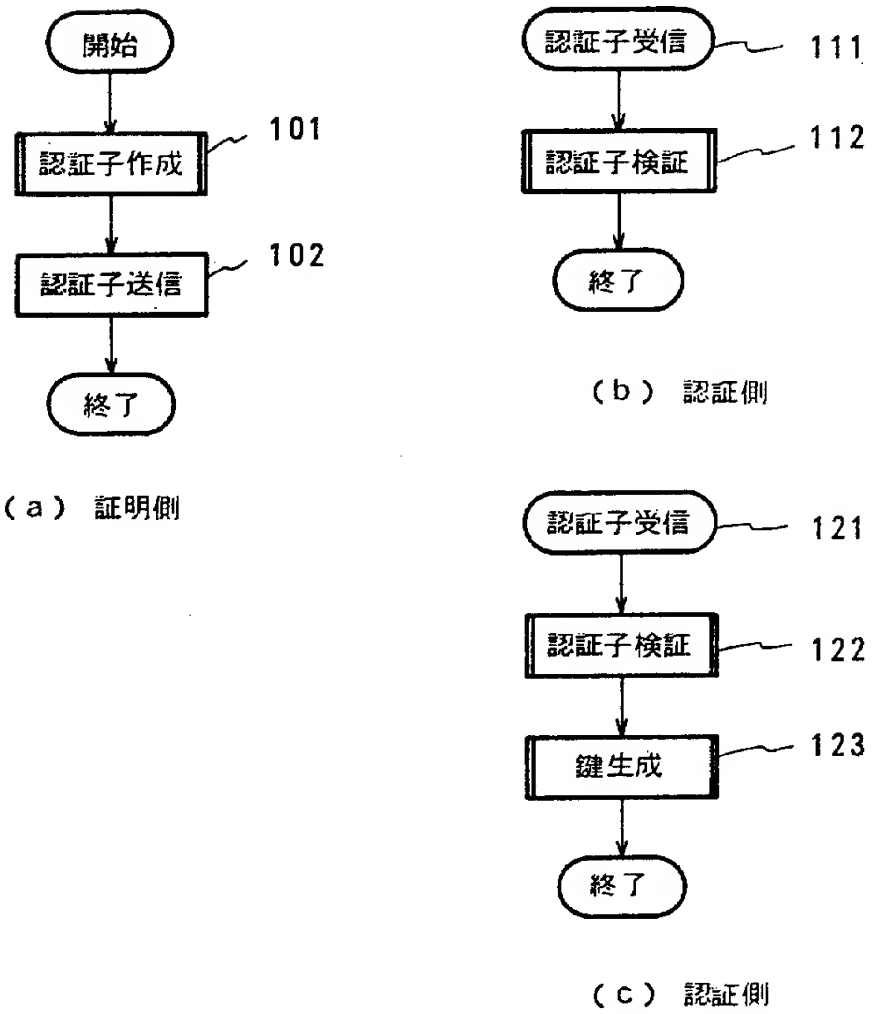
以上、詳細に説明したように、本発明を用いれば第３者による不正再送を防ぎ、あるいは暗号用の鍵生成も行なえるという機能付きの認証が実行できるのでネットワーク通信などに有用である。

図面の簡単な説明

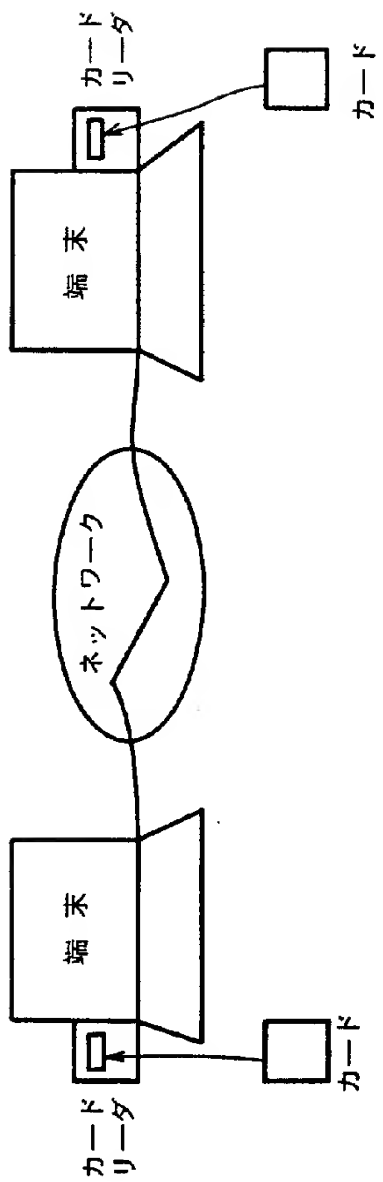
第１図は本発明の作用・原理を示す流れ図、第２図は本発明の実施例を示す構成図、第３、４、５図は第１図の認証子作成、認証子検証、鍵生成の各実施例を示す図である。図において、１０１は認証子作成機能、１０２は認証子送信機能を、１１１、１２１は認証子受信状態を、１１２、１２２は認証子検証機能を、１２３は鍵生成機能を各々を示す。

代理人　弁理士　内原　晋

第　1　図



第 2 図



第 3 図

認証子生成

① 乱数 r 生成

② $x=\alpha^{er} \pmod n$

③ c=hash(Time, x, Data)

④ $y=s\cdot\alpha^{cr} \pmod n$

第 4 図

認証子検証

① c=hash(Time, x, Data)

② $ID \neq y^e/x^c \pmod n$

なら不正データと判断

第 5 図

鍵生成

$wk=x^R \pmod n$